UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The person of Kya NELSON (DOB: XX/XX/2001) and the residence located at 4103 Saint Claire St, Racine, WI, as more fully described in Attachments A-1 & A-2

Case No. 21 MJ 65

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachments A-1 and A-2

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1030	Fraud and related activity in connection with computers
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Jeremy Durk
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: January 28, 2021

Judge's signature

City and state: Milwaukee, WI

U.S. Magistrate Judge William E. Duffin
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jeremy Durk, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 4103 Saint Claire St, Racine, Wisconsin (the "SUBJECT PREMISES") described in Attachment A-1, and the person of KYA NELSON ("NELSON") as described in Attachment A-2, for the things described in Attachment B.

2. I am a Special Agent ("SA") with the Federal Bureau of Investigation and have been so employed since September 2020. I presently am assigned to work a variety of criminal and national security matters, including the investigation of cybercrimes. I have worked in the field of information technology for approximately seven years, and have extensive experience with computers, databases, and network infrastructure.

3. This affidavit is based upon my personal observations, my training and experience, review of FBI records and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

PROBABLE CAUSE

4. Since November 17, 2020, FBI agents in Los Angeles have been investigating a nationwide series of "swatting" incidents involving the use of Ring LLC ("Ring")[1] smart doorbells.[2] Evidence collected by the FBI shows that the subjects responsible for the swatting (the "swatters") gained unauthorized access to the Ring and Yahoo email accounts of their victims and used that access to facilitate the swatting of the victims, and to stream it live on the internet. The FBI is investigating suspected criminal violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030 (Fraud and related activity in connection with computers), and 18 U.S.C. § 1028A (Aggravated Identity Theft).

5. Swatting is a harassment technique in which swatters falsely report a threat (for example, a bomb threat, an active shooter, or a hostage situation) to law enforcement in an attempt to provoke an emergency response, including deployment of tactical and emergency service response teams, to the swatting target's address. Depending on the nature of the false threat, law enforcement will sometimes arrive with a Special Weapons and Tactics ("SWAT") team, armed with specialized weapons and equipment. Swatting can result in the evacuations of schools, businesses, and homes and is often done to harass and intimidate the target(s).

---

[1] Ring LLC is a home security and smart home company owned by Amazon.

[2] A smart doorbell is an internet connected doorbell that can be accessed remotely by a user through a website. Many smart doorbells, including Ring devices, have cameras that their owners can use to see what is in the device's field of vision and microphones that owners can use to speak with people near the doorbell.

6. On or about November 14, 2020, Ring contacted the FBI in Los Angeles to report multiple incidents of swatting that involved the use of Ring smart doorbells. Ring provided a variety of information, further discussed below, to the FBI. Ring indicated that swatters had gained unauthorized access to multiple customer accounts and doorbell devices.

7. On or about November 17, 2020, I received some information about a swatting incident in Huntsville, Alabama on November 12, 2020. Based on my review of a Huntsville Police Department ("HPD") report and communications with HPD officers, I learned the following:

a. On November 12, 2020, HPD received a call from telephone number 702-500-2126 number (the "2126 number") in which the caller claimed to be a 13-year-old female who said that her father, N.D., had shot her mother at a home on Pentelope Drive.

b. A short time later HPD received a call from telephone number 304-774-5907 (the "5907 number") in which a male caller said that he lived on Pentelope Drive, and that he had heard gunshots coming from his next-door neighbor's house.

c. HPD officers arrived at the home on Pentelope Drive identified by the first caller. The officers contacted a man and woman and ordered them out of the house at gunpoint. Officers then determined that there was no problem at the home, and that the reported crimes did not occur. Officers also determined that there was nothing amiss at the home next door to the second caller's supposed address.

d. N.D. told HPD that he had heard talking on his Ring smart doorbell shortly before the HPD officers arrived. He discovered that the doorbell seemed to have been hacked and he could hear people talking through the speaker on the camera. N.D. said he had unplugged the doorbell and taken it inside the house.

e. HPD Officer James Leonard entered the home and could hear a male voice coming from the Ring device. Officer Leonard identified himself, and the voice on the Ring claimed that his name was "Chum" and that he was from Chicago.[3] He admitted that he had hacked the doorbell and called the police. Chum then threatened to get Officer Leonard's social security number before ending the communication through the doorbell shortly thereafter.

f. Officer Leonard called the 5907 number, and a man answered. Officer Leonard believed it to be the same "Chum" he had spoken with through the Ring doorbell. The man claimed to engage in swatting for entertainment, and that he was part of a group who used leaked account credentials to gain access to doorbells. He claimed to have a website called chumscam.com where his group streamed videos of swatting.

8. On or about November 17, 2020, I received a list of IP addresses[4] identified by Ring as having been used to illegally access their customers' Ring accounts, and a spreadsheet

---

[3] The SUBJECT PREMISES is located approximately 75 miles from Chicago.

[4] Based on my training and experience, I know that an Internet Protocol version 4 address, also known as an "IPv4 address," or more commonly "IP address," is a set of four numbers, each ranging from 0 to 255 and separated by a period (".") that is used to route traffic on the internet. A single IP address can manage internet traffic for more than one computer or device, such as when a router in one's home routes traffic to

identifying the internet service provider ("ISP") and approximate geographical location associated with each IP address. I determined that most of the IP addresses were associated with virtual private network ("VPN") providers or proxies, which conceal the true IP address of the computer accessing the site, however a few appeared to originate from standard ISPs, suggesting that they were the real IP addresses of the individuals who accessed the Ring accounts.

9. On or about November 17, 2020, I received, from a Ring employee, a document detailing 14 swatting incidents that Ring was aware of, along with supporting materials. From those materials, I learned the following:

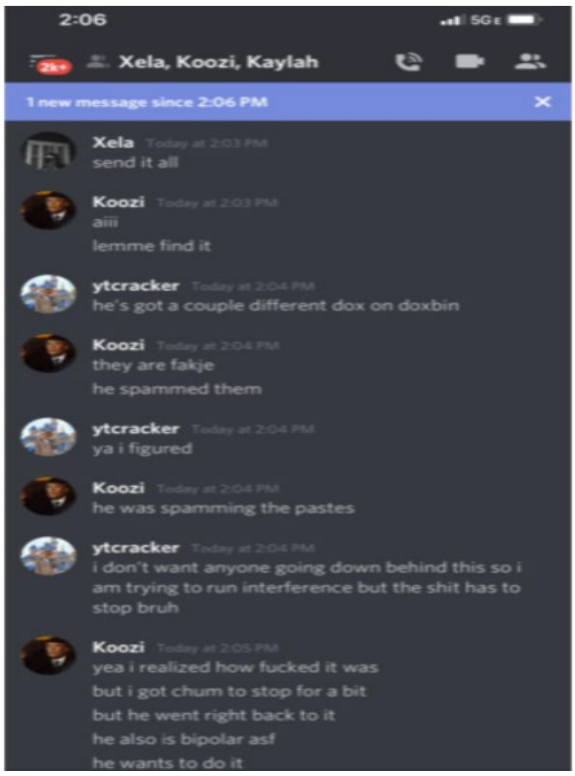
a. Ring identified three user accounts on the instant messaging and voice chat platform Discord[5] that it believed were connected to the swatting incidents: **Koozi#0001**, **luci <$#0064**, and **Chumlul#1421**.

---

one's desktop computer, as well as one's tablet or smartphone, while all using the same IP address to access the internet. Use of a common IP address can, at times, show the use of shared or common computer infrastructure or use of the same physical space to connect to the internet.

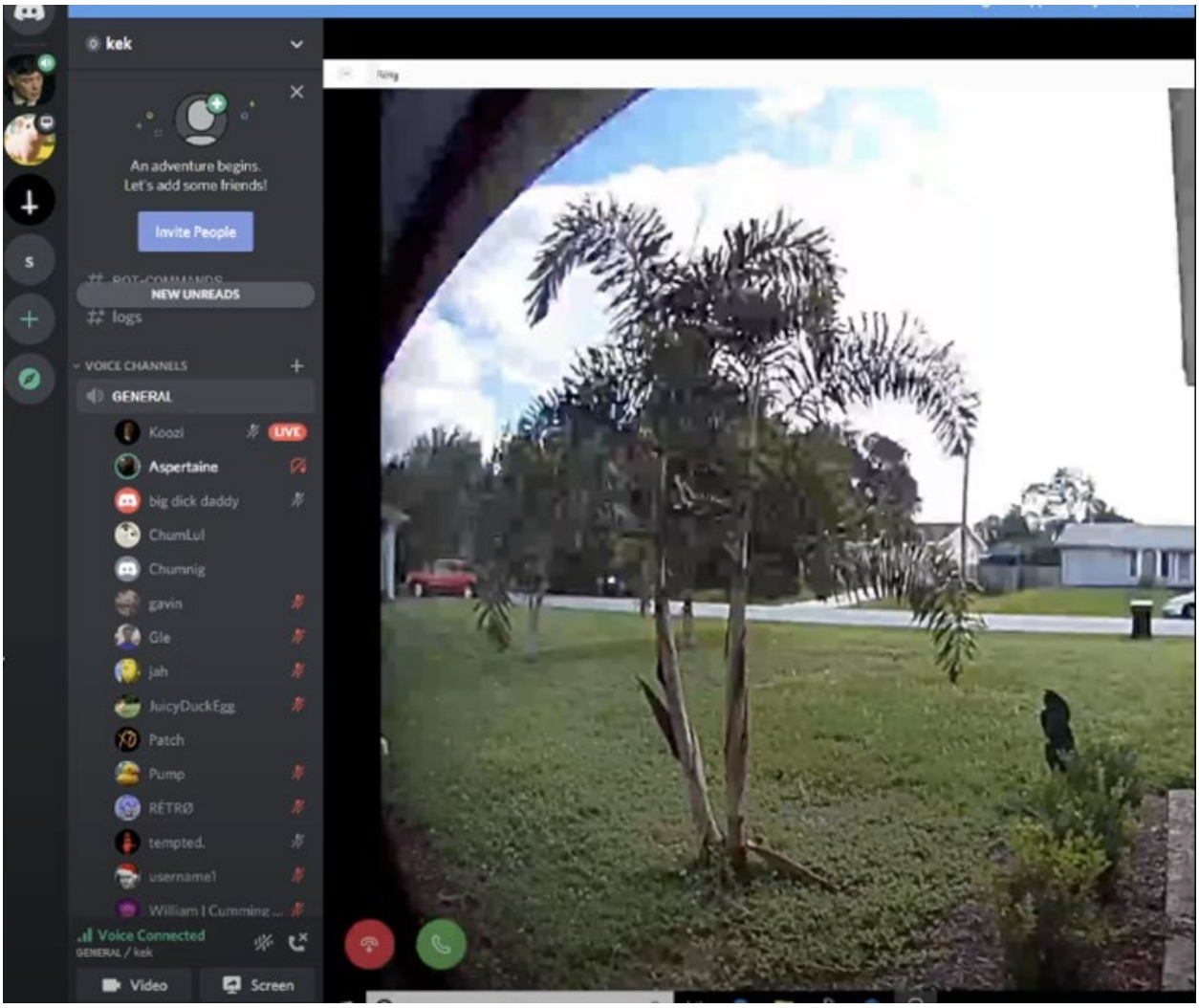
[5] Discord is an online communication platform that allows users to create private virtual communication servers that can be shared with others. On those servers, users can create dedicated audio, video, and text communication channels, and users are able to join or connect to those channels to communicate. Discord also supports live streaming of video from a user device. Discord channels are similar to a chat room, in that the users are able to share real-time audio, video, and text messages with other participants in the channel. Discord users are also able to send one-to-one direct messages with other users.

b. A Ring employee, operating in an undercover capacity, and using the name ytcracker, engaged in the following communications with **Koozi#0001** on Discord, where **Koozi#0001** discussed being involved in swatting with "Chum"**:**



c. In the above chat, discussing swatting, **Koozi#0001** said among other things, "I got chum to stop for a bit [¶] but he went right back to it."

10. On or about November 18, 2020, an employee of Discord contacted me to make an emergency disclosure of information about accounts tied to the swatting incidents. The information provided by Discord included account details for the three previously identified accounts, and a fourth account that Discord had identified: **Aspertaine#1**. Discord also provided a screenshot from the streaming video of a swatting incident in North Port, Florida:



11. The screenshot provided by Discord shows that **Koozi#0001**, **Chumlul#1421**, and **Aspertaine#1**,[6] among others, participated in the live stream of the swatting.

12. On or about December 1, 2020 I conducted open source research for the email address used to register the Discord account **Chumlul#1421**. The same email account, **cupcake14200@gmail.com**, was used to register a Skype account with the display name Kya Nelson.

13. On or about November 19, 2020 I analyzed the login IP addresses provided by Discord for **Chumlul#1421** and the login IP addresses that Ring identified as having been used to gain unauthorized access to customer accounts and devices. Through that analysis, I identified IP address **75.86.95.8** as having been used to log in to both Ring customer accounts and to the **Chumlul#1421** account.

a. Charter Communications records for IP address **75.86.95.8** show that it was assigned to an account at 4103 Saint Clare St, Racine, Wisconsin (the SUBJECT PREMISES). The account lists the phone number 262-417-4877 (The "4877 number").

---

[6] On December 17, 2020, the FBI executed a search warrant at the Arizona residence of James McCarty, the user of the **Aspertaine#1** account. In a recorded interview with the FBI, after being advised of his *Miranda* rights, McCarty admitted to using the **Aspertaine#1** Discord account and participating in some of the Ring swatting incidents. McCarty identified Koozi and Chum as participants in the Ring swatting incidents. McCarty claimed not to know anything about Chum's identity, but said that Chum did not use a VPN to log into the hacked Ring accounts. This is consistent with my observation of logins from the IP address associated with the SUBJECT PREMISES to both the **Chumlul#1421** Discord account and the Ring accounts of swatting victims.

b. Discord records show that the 4877 number was also used to register the **Chumlul#1421** Discord account.

c. On or about December 1, 2020, I received records from T-Mobile for the 4877 number showing that the subscriber was Erik Nelson. On December 3, 2020 I conducted social media research on Erik Nelson and located a Facebook account for E. Nelson which identified Kya Nelson as one of his sons. The account also included a celebration of Kya Nelson's 18th birthday on October 29, 2019—which is consistent, as discussed below, with other records related to Kya Nelson.

14. On or about November 18, 2020, Ring sent me information about a tweet from Twitter account @Chum23617263 about the Ring swatting incident in North Port Florida described above. The user of @Chum23617263 responded to a tweet about the incident, saying "haha, me and my friends did this."

a. Twitter records show that the account @Chum23617263 was registered with Twitter from IP address of 75.86.95.8, the IP address associated with the SUBJECT PREMISES.

15. On or about November 19, 2020, I received information about a swatting incident in West Covina, California on November 8, 2020. Based on my review of the West Covina police report, I learned the following:

a. On November 8, 2020, West Covina police received a call from the 2126 number, which was also used in the Huntsville, Alabama swatting discussed in paragraph 7 above. The caller claimed to be a 14-year-old female (J.T.) who said that her mother C.T., and her father B.T.

were both under the influence of alcohol and were playing with guns. The caller further stated that both of her parents were shooting the guns inside the house.

b. West Covina dispatch received a second phone call from 414-909-9123 (the "9123 number") in which the caller claimed to be "Josh," a friend of the C.T. and B.T.'s family who had left the location when he saw that they were pulling out guns.

c. West Covina Police Officer Canton arrived at the location identified by the first caller, where a male and a female (R.Z. and C.Z.) met him and stated they did not own any weapons.

d. When Officer Canton approached the front door, the Ring doorbell activated and a male voice began to say over the camera he was going to kill everyone and that he would shoot anyone that entered the house. Another female voice joined in repeatedly saying "fuck the police."

e. As officers searched the residence, the Ring camera activated again and started to play NWA's "Fuck the Police."

f. Officers ultimately concluded that there were no signs of the reported shooting, and that R.Z. and C.Z. were victims of swatting.

16. On December 1, 2020, I received records from TextNow for the 9123 number. Those records showed that the number was registered under the name Kya Nelson, with email address kyanelson1420@gmail.com, from IP address 75.86.95.8 – the same IP address associated with the SUBJECT PREMISES.

17. As part of my investigation, I monitored communications on the Discord chat platform. On or about November 27, 2020, I observed an account named **Chum#0212** (with moniker "Chum Legend") boast of hacking Ring accounts and swatting the owners of those accounts. The user of the account also claimed that he or she was 19 years old. I observed the following chat involving **Chumlul#1421**:

18. Based on my research into Discord and my experience monitoring the subjects involved in this case, I believe that the user of the **Chum#0212** account was the same person who used the **Chumlul#1421** account. Discord users often create alternative accounts with similar usernames when their previous accounts are banned by Discord (for example, for violations of the terms of use of the service).

19. Discord records show that the **Chum#0212** account was registered from IP address 75.86.95.8 the IP address associated with the SUBJECT PREMISES and which was also used to register the **Chumlul#1421** account.

20. On or about December 4, 2020 I submitted a Wisconsin Department of Motor Vehicles ("DMV") record request relating to Kya Nelson, which returned his last known address as 4103 Saint Clare St, Racine, Wisconsin (the SUBJECT PREMISES). They also showed that he was 19 years old (the same age **Chum#0212** claimed to be).

21. I also conducted research to identify any other potential residents of the SUBJECT PREMISES. DMV records for Nelson's brother show that he used the SUBJECT PREMISES as his address, however social media posts connected to Nelson's brother indicate that the brother does not live at the SUBJECT PREMISES and is now located in Colorado. Queries to the Accurint public records database suggest that at least one other person may have recently resided at the SUBJECT PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

22. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

23. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe the records sought will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users

typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer

accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware

and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

27. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those

computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

28. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A-1 and the person of KYA NELSON described in Attachment A-2, and seize the items described in Attachment B.

ATTACHMENT A-1

Property to be searched

The property to be searched is a residence located at 4103 Saint Claire St, Racine, Wisconsin, including any and all storage units, containers, safes, automobiles, carports, garages, and outbuildings (the "SUBJECT PREMISES"). The SUBJECT PREMISES, pictured below, is a grey and tan building with a red roof and a white door. The building is a duplex that is split in two with each side having a different address. Half of the building is the SUBJECT PREMISES and is assigned the address 4103.

ATTACHMENT A-2

Person to be searched

The person of KYA NELSON ("NELSON"), date of birth October 29, 2001, height 5'8" with blond hair and hazel eyes. The search of NELSON shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within NELSON's immediate vicinity and control at the location where the search warrant is executed. The search shall not include a strip search or a body cavity search.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030 (Fraud and related activity in connection with computers), and 18 U.S.C. § 1028A (Aggravated Identity Theft) (the "SUBJECT OFFENSES"), those violations involving KYA NELSON and occurring after July 1, 2020, including:

a. Records and information related to a conspiracy to engage in swatting;

b. Records and information related to any swatting incidents, including but not limited to photographs, videos, drawings, depicting the likenesses of any victims, their relatives, neighbors, co-workers, or friends;

c. Records and information related to communications with and the identity of any victims of swatting or aggravated identity theft;

d. Records and information related to accessing Ring doorbells, including but not limited to login and password information for Ring accounts;

e. Records and information related to unauthorized access to online accounts of others, including but not limited to login and password information for accounts;

f. Records and information related to any victims of swatting or aggravated identity theft, or their relatives, neighbors, co-workers, students, or friends, including their names, addresses, phone numbers, location information, contact information, or any other personal identifying information or information about their places of work, school, or residence;

g. Records and information relating to the purchase, possession, or use of digital devices, including smartphones, "burner" phones, desktop computers, laptop computers, encryption software/services, virtual Private Network ("VPN") subscription services, and identity alteration or modulation devices, programs and software;

h. Records and information relating to accounts used or controlled by NELSON with any telephone service provider, internet service provider, or other online communication service, including but not limited to Bandwidth, TextNow, and Charter Communications;

i. Records and information related to the use of instant and social media messages (such as Discord, Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device in connection with the SUBJECT OFFENSES;

j. Records and information related to call logs, including all telephone numbers dialed from any of the digital devices found at the SUBJECT PREMISES and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

k. Records and information sufficient to show address book information, including all stored or saved telephone numbers;

l. Records and information sufficient to show indicia of occupancy, residency or ownership of the SUBJECT PREMISES and the property to be seized pursuant to

the warrants, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease of rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

m. Records and information relating to the identity or location of the suspects; and

n. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations.

2. Computers or storage media used as a means to commit the violations described above, including unauthorized access to protected computers in violation of 18 U.S.C. § 1030(a)(2) and aggravated identity theft in violation of 18 U.S.C. § 1028A.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.